Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology

Application Deployment Certification Policy

I. **Statement**

Any computer applications must undergo a battery of tests to determine if it is suitable to be deployed into production. Based on the test results, the Chief Information Officer (CIO) makes the final determination whether or not this application should be placed into production.

II. **Purpose**

As applications have become more complex, more interconnected, and more exposed to the external world, it has become even more important to thoroughly vet them before they are deployed into production. This policy establishes a uniform and objective battery of tests that enables the CIO to evaluate the suitability of an application to be deployed into production.

III. **Applicability**

This policy applies both to new applications as well as modifications to existing applications. It covers:

1. Executive Branch and *Semi-autonomous State Agencies*[1], irrespective of where their applications are hosted; and
2. Applications from other State government branches that are hosted on devices operated by the Office of Information Technology, or those that traverse the State's wide area network.

IV. **Responsibilities**

A. *Application Owners*[2]: The Application Owners are responsible for executing this test battery and submitting the results to the Director, Project Management Office (PMO). This submission consists of:

1. The names and signatures of the Project Manager, the Product Manager, and the Executive Sponsor; and
2. A summary result (Passed/Failed/Not Applicable) and a short paragraph clarifying that summary result, for each of the tests specified below.

[1] See Definition[4]
[2] See Definition[1]

Any part of the testing may be outsourced to a third-party without affecting the responsibility or the prerogative of the Application Owners. Irrespective of who actually executes a test, the Application Owners still remain in charge of its execution. The Application Owners are not answerable to the third-party regarding the nature or the result of any outsourced test. Further, the third-party exclusively conveys the test results back to the Application Owners, and never directly to the Director, PMO.

B. Chief Information Officer (CIO): The CIO may delegate authority to certify or approve applications for deployment. Regardless of approving authority, certification of applications will be based on advice from the Director, PMO, the Chief Technology Officer (CTO), the Associate CIO for Applications, and/or other subject matter experts.

C. Director, PMO: This Policy is owned, interpreted, executed, and enforced by the Director, PMO.

V. **Directives**

A. The following list defines the battery of application tests:

1. *Use Cases*[3] Test: Ensures proper functioning of all the features of the application.
2. Accessibility Test: Ensures compliance with the Maine I.T. accessibility policies and standards.
3. Data Conversion Test: Ensures the accurate migration of appropriate legacy data.
4. Interfaces Test: Ensures proper functioning with all companion applications.
5. Security Test: Ensures the confidentiality, integrity, and availability of the application.
6. Performance Test: Ensures responsiveness under projected average and peak processing loads.
7. Restoration Test: Ensures full functioning of the application following an infrastructure rollback/restoration.
8. Regression Test: Applies exclusively to modifications of existing applications. Ensures that a new version does not compromise existing functionality.

B. Brief general descriptions of the tests are provided below:

1. Use Cases Test: An application must have a complete, stable, and up-to-date documentation of the full set of its Use Cases. Each of the Use Cases must be executed individually, and verified that it indeed delivers as expected. Beyond individual Use Cases, Application Owners must also know which Use Cases are likely to be invoked simultaneously with one another. All such likely combinations of Use Case interactions must be tested. Finally, it is also important to test a representative sample of actual end-users performing their daily jobs holistically, using the entirety of an application. At the completion of the Use Cases Test, the end-users must be satisfied that the application does indeed meet all their expectations, or alternatively, that they are willing to accept any deficiencies thereof. At the discretion of the Director, PMO, alternative requirements definition artifacts may be acceptable in lieu of Use Cases.

[3] See Definition[5]

2. Accessibility Test: The application must be tested to ensure its compliance with the State I.T. accessibility policies and standards[4].

3. Data Conversion Test: It is likely that record structures and formats of the legacy application were modified as a result of the migration into the new application. It must be ensured via actual testing that all business-critical data have indeed survived the migration. It is left to the discretion of the Application Owners to determine exactly what constitutes 'business-critical data.' But once so determined, it must be ensured that such data are indeed accessible from the new application. Should the new application precipitate modifications to the existing workflows, then this step must also include testing the new workflows.

4. Interfaces Test: An application must have a complete and up-to-date documentation of all the data and workflow dependencies between itself and all other applications that it interacts with. All such interactions must be tested. Interfaces must anticipate errors, and therefore, incorporate robust error-handling and error-logging capabilities. While it is desirable to exclusively utilize the Test environments of the various applications when testing the interfaces, it may be necessary under certain circumstances to pair the Test environment of this application with other environments of companion applications, as long as such other applications participate in the interface on a read-only basis.

5. Security Test: The application must ensure the highest levels of Confidentiality (No unauthorized access), Integrity (No tampering), and Availability (No denial-of-service). All personal, medical and financial data, in motion, must be encrypted end-to-end, both inside and outside the State firewall. All personal, medical, and financial data must be encrypted at rest in the Demilitarized Zone. Data hosted on servers inside the firewall are not subject to encryption, but data resident in portable computing devices must be encrypted at all times. A full vulnerability assessment and penetration test must be performed on the application. Applications should not only guard against standard security vulnerabilities (such as Weak Credentials, Injection Attacks, Buffer Overflows, Cross-site Scripting, etc.), but they should also be designed to thwart denial-of-service attacks. Beyond such generic requirements, an application may also need to satisfy additional specific, statutory requirements, as set forth by CJIS, HIPAA, FISMA/FIPS, SOX, GLBA, CROMERR, USA Patriot Act, etc. The Enterprise Security Office will provide further guidance on this item, as needed.

6. Performance Test: Performance determines the responsiveness of the application to its users, and therefore, its acceptance and adoption. The application must respond adequately under the projected average load, as well as the peak processing load. The application must not cause unreasonable adverse impact on either network throughput or server loading. Network throughput is a function of many different factors, viz., the loading on the network, settings on switches and routers, size of the transactions, payload-to-overhead ratio, etc. For the purpose of this Policy, network throughput will be measured by combining the payload-to-overhead ratio with transaction size, under very low server load conditions. The

[4] http://www.maine.gov/oit/accessibility/policy/index.html

application should tune the following two factors in its control to affect this measurement: the screen buffer size and the transaction size. In order to safeguard against adverse user perception, the application must establish a two-tiered response time specification, one for data inquiry/lookup, and another for data modification transactions. For load tests, the application may consider using automated tools that simulate user behavior, including simultaneous and staggered loading. Beyond response times, other aberrations that must be investigated include non-linear performance, i.e., response time increasing disproportionately with loading, and response time varying during periods of constant load. This is a test that requires close cooperation with the hosting provider.

7. Restoration Test: Subsequent to a point-in-time recovery of the entire suite of application components (the client-device, the webserver, the application server, the file server, and the database server), the application must be tested to ensure that it functions exactly as expected. It is left to the discretion of the Application Owners to determine whether that constitutes the entire suite of Use Cases or merely a core suite of essential Use Cases. Either way, the endgame is to ensure that the application functions entirely to the satisfaction of its end-users following an infrastructure rollback/restoration. Equally important is to negotiate with the infrastructure provider the two metrics of recovery: *Recovery Point Objective*[5] and *Recovery Time Objective*[6]. This is a test that requires close cooperation with the hosting provider.

8. Regression Test: This test applies whenever there is a modification to an existing application, either an upgrade to the application proper, or an upgrade to an embedded, third-party component. This is to ensure that the modification did not adversely affect previously working functionality. A two-pronged regression test strategy must be undertaken. Based upon the release notes and the known module dependencies, a focused test suite must be administered for those Use Cases that are actually affected as part of this upgrade. At the same time, a core suite of essential functions must also be tested, irrespective of whether or not they underwent any modification as part of this upgrade. It is left to the discretion of the Application Owners to determine exactly what constitutes a 'core suite of essential functions.' Such a two-pronged strategy provides failover protection against fallibility of release notes and incomplete knowledge of module dependencies.

C. Besides the battery of application tests described above, the application must be deployed onto pre-certified infrastructure, as defined by the Infrastructure Deployment Certification Policy[7].

VI. **Definitions**

1. Application Owners: With respect to the application being considered for deployment, the Project Manager, the Product Manager, and the Executive Sponsor are jointly and collectively identified as the Application Owners. If, for any reason, any of the roles

[5] See Definition[2]
[6] See Definition[3]
[7] http://maine.gov/oit/policies/InfraDeployCert.htm

turns out to be vacant, or the same person fulfils more than one role, or there arises a difference-in-opinion with respect to this Policy among the three roles, for the purpose of this Policy, the decision of the Director, PMO, will be final and binding.

2. Recovery Point Objective: The Recovery Point Objective is the point-in-time *to which* an application must be restored subsequent to a disaster or disruption.

3. Recovery Time Objective: The Recovery Time Objective is the duration-of-time *within which* an application must be restored subsequent to a disaster or disruption.

4. Semi-autonomous State Agency: An agency created by an act of the Legislature that is not part of the Executive Branch. This term does not include the Legislature, the Judiciary, the Office of the Attorney General, the Office of the Secretary of State, the Office of the State Treasurer, and the Audit Department.

5. Use Case: A Use Case is a well defined sequence of actions undertaken jointly by the user and the application, which produces a predictable result of value to the user. Thus, a Use Case captures a discrete functionality of an application completely independent of the underlying implementation. Beyond the expected outcomes, a Use Case must anticipate errors, and therefore, incorporate robust error-handling and error-logging capabilities. The full set of all the Use Cases for an application constitutes the complete value added by that application.

VII. **References**

1. Software Development Lifecycle Policy[8]

2. Hosting Location Policy[9]

3. Remote Hosting Policy[10]

4. Policy to Safeguard Information on Portable Computing and Storage Devices[11]

5. Change Management Standard[12]

6. Infrastructure Deployment Certification Policy[13]

VIII. **Document Information**

Adoption Date: September 22, 2010
Effective Date: September 22, 2010
Last Revision Date: August 5, 2013 – to update enforcement only.
Next Revision Date: August 5, 2015

[8] http://maine.gov/oit/policies/SDLCPolicy.htm
[9] http://maine.gov/oit/policies/hostinglocationpolicy.htm
[10] http://maine.gov/oit/policies/Remote-Hosting-Policy.htm
[11] http://maine.gov/oit/policies/SafeguardingPolicy_Final.htm
[12] http://maine.gov/oit/policies/ChangeManagementStandard.htm
[13] http://maine.gov/oit/policies/InfraDeployCert.htm

Point of Contact: B. Victor Chakravarty, Enterprise Architect, Office of Information Technology, 207-624-9840.

Approved By: James R. Smith, Chief Information Officer, Office of Information Technology, 207-624-8800.

Position Title(s) or Agency Responsible for Enforcement: Doug Birgfeld, Director, Project Management Office, Office of Information Technology, 207-624-9793.

Legal Citation: 5 M.R.S.A. Chapter 163 Section 1973 paragraphs (1)B and (1)D, which read in part, "The Chief Information Officer shall:" "Set policies and standards for the implementation and use of information and telecommunications technologies…" and "Identify and implement information technology best business practices and project management."

Waiver Process: See the Waiver Policy[14].

[14] http://maine.gov/oit/policies/waiver.htm